1. GCDs, redux
   (a) Prove that if \(d = \text{G.C.D.}(a, b)\), then \(d \mid (ax + by)\) for any \(x, y \in \mathbb{Z}\).
   (b) Find \(x, y \in \mathbb{Z}\) such that \(49x + 100y = 1\).
   (c) Prove that if \(\text{G.C.D.}(a, n) = 1\), then the congruence \(ax \equiv b \pmod{n}\) has a solution.
   (d) Find (and prove) conditions on \(a, b, n\) that guarantee solutions to the congruence \(ax \equiv b \pmod{n}\) even if \(\text{G.C.D.}(a, n) > 1\).
   (e) Show that if \(\text{G.C.D.}(a, n) = 1\), then \(a\) has a multiplicative inverse in the \(\mathbb{Z}_n\) system.
   (f) Find the multiplicative inverse of 53 in \(\mathbb{Z}_{79}\) by reversing the Euclidean Algorithm.
   (g) For which \(n\) does \(2\) have a multiplicative inverse in \(\mathbb{Z}_n\)?
   (h) For which \(n\) does \(4\) have a multiplicative inverse in \(\mathbb{Z}_n\)?
   (i) For which \(n\) does \(6\) have a multiplicative inverse in \(\mathbb{Z}_n\)?

2. Prime Factorizations
   (a) Use the Sieve of Eratosthenes to find all primes up to 200.
   (b) Find the prime factorization of all positive integers \(\leq 200\).
   (c) What is the smallest integer that has no prime factors less than 17?
   (d) If you wanted to determine all prime less than or equal to 1000, what is the largest primes you would need to sieve by?

3. Primes
   (a) Let \(p\) be a prime. Show that if \(p \mid a\), then \(\text{G.C.D.}(p, a) = p\), but if \(p \nmid a\), then \(\text{G.C.D.}(p, a) = 1\).
   (b) Show that if \(p\) is prime and \(p \mid (ab)\), then \(p \mid a\) or \(p \mid b\) (or both!).
   (c) Show by example that if \(n\) is not prime, then it is possible for \(n \mid (ab)\) without either \(n \mid a\) or \(n \mid b\).
   (d) Show that there are infinitely many primes of the form \(4n + 3\).
   (e) Show that there are infinitely many primes of the form \(6n + 5\).

4. Fun with Small Primes
   (a) Show that if \(m\) is odd, then \(m^2 \equiv 1 \pmod{2}\).
   (b) Show that if \(m\) is odd, then \(m^2 \equiv 1 \pmod{4}\).
   (c) Show that if \(m\) is odd, then \(m^2 \equiv 1 \pmod{8}\).
   (d) Show that if \(m \in \mathbb{Z}\), then \(m^3 \equiv m \pmod{3}\).
   (e) Show that \(3 - 5 - 7\) is the only set of three “consecutive” primes. (Obviously, all primes besides 2 are odd, so “consecutive” in this case means among odd numbers.)